



2.4GHz 11 Mbps Wireless Bridge

User Guide

SMC2582W-B

Copyright

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Copyright © 2003 by
SMC Networks, Inc.
38 Tesla
Irvine, California 92618
All rights reserved.

Trademarks

SMC is a registered trademark; and EliteConnect is a trademark of SMC Networks. Other product and company names are trademarks or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, (example — use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada - Class B

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of Industry Canada.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques," NMB-003 édictée par l'Industrie.

EC Conformance Declaration - Class B

SMC contact for these products in Europe is:

SMC Networks Europe,
Edificio Conata II,
Calle Frutuós Gelabert 6-8, Planta 2,
08970 - Sant Joan Despí,
Barcelona, Spain.

This RF product complies with R&TTE Directive 99/5/EC (Annex IV) and with the requirements of the Council Directive 89/336/EEC on the Approximation of the laws of the Member States relating to Electromagnetic Compatibility and 73/23/EEC for electrical equipment used within certain voltage limits and the Amendment Directive 93/68/

EEC. For the evaluation of the compliance with these Directives, the following standards were applied:

- Electromagnetic compatibility and radio spectrum matters (ERM) EN300 328-1 (2001-12) and EN300 328-2 (2001-12)
- Electromagnetic Compatibility (EMC) Standard for radio equipment and services EN301 489-1 and EN301 489-17
- Safety Test EN60950
- Immunity to conducted disturbances, Induced by radio-frequency fields EN 61000-4-6:1996 (0.15 - 80 MHz with 1 kHz AM 80% Modulation: 3 V/m)
- Power frequency magnetic field immunity test according to EN 61000-4-8:1993 (1 A/m at frequency 50 Hz)
- Voltage dips, short interruptions and voltage variations immunity test according to EN 61000-4-11:1994 (>95% Reduction @10ms, 30% Reduction @500 ms, >95% Reduction @5000 ms)
- LVD: EN 60950 (A1/1992; A2/1993; A3/1993; A4/1995; A11/1997)
- MDD: IEC 60601-1

Wichtige Sicherheitshinweise (Germany)

1. Bitte lesen Sie diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den späteren Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwenden Sie keine Flüssig- oder Aerosolreiniger. Am besten eignet sich ein angefeuchtetes Tuch zur Reinigung.
4. Die Netzanschlußsteckdose soll nahe dem Gerät angebracht und leicht zugänglich sein.
5. Das Gerät ist vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sicheren Stand zu achten. Ein Kippen oder Fallen könnte Beschädigungen hervorrufen.
7. Die Belüftungsöffnungen dienen der Luftzirkulation, die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.

8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollte auch nichts auf der Leitung abgestellt werden.
10. Alle Hinweise und Warnungen, die sich am Gerät befinden, sind zu beachten.
11. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
12. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. elektrischen Schlag auslösen.
13. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von autorisiertem Servicepersonal geöffnet werden.
14. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
 - a. Netzkabel oder Netzstecker sind beschädigt.
 - b. Flüssigkeit ist in das Gerät eingedrungen.
 - c. Das Gerät war Feuchtigkeit ausgesetzt.
 - d. Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
 - e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
 - f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
15. Stellen Sie sicher, daß die Stromversorgung dieses Gerätes nach der EN60950 geprüft ist. Ausgangswerte der Stromversorgung sollten die Werte von AC 7,5-8V, 50-60Hz nicht über- oder unterschreiten sowie den minimalen Strom von 1A nicht unterschreiten. Der arbeitsplatzbezogene Schalldruckpegel nach DIN 45 635 Teil 1000 beträgt 70dB(A) oder weniger.

1. Introduction

1.1. Overview

The SMC2582W-B is a versatile device that can be configured to be in one of the 3 operational modes—Access Point, Bridge Master, and Bridge Slave—for various wireless bridging applications. With the convenient Web-based user interface, a network administrator can easily and clearly manage the SMC2582W-B.

In Chapter 2, we describe the steps to install and configure a newly acquired SMC2582W-B. Following the steps, the SMC2582W-B can be quickly set up to work. In Chapter 3, detailed explanation of each Web management page is given for the user to understand how to fine-tune the settings of an SMC2582W-B to meet his or her specific needs.

1.2. Features

• IEEE 802.11b

• Operational modes.

- **Access Point.** The AP enables IEEE 802.11 Stations (STAs) to automatically associate with it via the standard IEEE 802.11 association process. In addition, the IEEE 802.11 WDS (Wireless Distribution System) technology can be used to manually establish wireless links between two APs or between an AP and a Bridge Master.

- **Bridge Master.** Use this mode to provide the Bridge Master functionality of the SMC2682W. The Bridge Master mode is designed to work in those networks where SMC2682W Wireless Bridge Slaves are already installed. The Bridge Master enables Bridge Slaves to automatically associate with it. It also enables IEEE 802.11 Stations, which are on the same LAN as the Bridge Master, to automatically associate with it via the standard IEEE 802.11 association process. In addition, the IEEE 802.11 WDS (Wireless Distribution System) technology can be used to manually establish wireless links between two Bridge Masters or between a Bridge Master and an AP.

- **Bridge Slave.** Use this mode to provide the Bridge Slave functionality of the SMC2682W. The Bridge Slave mode is designed to work in those networks where SMC2682W Wireless Bridge Masters are already installed.

- **64-bit and 128-bit WEP (Wired Equivalent Privacy).** For wireless data encryption.

- **Enabling/disabling SSID broadcasts.** When the SMC2582W-B is in AP or Bridge Master mode, the administrator can enable or disable the SSID broadcasts functionality for security reasons. When the SSID broadcasts functionality is disabled, an STA or Bridge Slave cannot associate with the AP or Bridge Master with an ANY network name (SSID, Service Set ID); the correct SSID has to be specified on the STA or Bridge Slave.

- **MAC-address-based access control.** When the SMC2582W-B is in AP or Bridge Master mode, it can be configured to block unauthorized STAs or Bridge Slaves based on MAC (Media Access Control) addresses. The ACL (Access Control List) can also be downloaded from a TFTP server.

- **Transmit power control.** Transmit power of the SMC2582W-B can be adjusted to control the area of coverage.

- **Link integrity.** When the SMC2582W-B is in AP or Bridge Master mode and the Ethernet LAN interface is detected to be disconnected from the wired network, all currently associated wireless clients (STAs and Bridge Slaves) are disassociated by the SMC2582W-B and no wireless client can associate with it thereafter.

- **Associated wireless clients status.** Showing the status of all wireless clients (STAs and Bridge Slaves) that are associated with the SMC2582W-B.

- **Detachable antenna.** The SMC2582W-B antenna can be replaced with high-gain antennas for long operating range.

- **DHCP client.** The SMC2582W-B can automatically obtain an IP address from a DHCP server.

- **DHCP server.** The SMC2582W-B can automatically assign IP addresses to computers or other devices by DHCP (Dynamic Host Configuration Protocol).

- **Static DHCP mappings.** The administrator can specify static IP address to MAC address mappings so that the specified IP addresses are always assigned to the hosts with the specified MAC addresses.

- **Showing current DHCP mappings.** Showing which IP address is assigned to which host identified by a MAC address.

- **Packet Filtering.** The SMC2582W-B provides Layer 2, Layer 3, and Layer 4 filtering capabilities.

- **Firmware Tools**

- **Firmware upgrade.** The firmware of the SMC2582W-B can be upgraded via the following methods:

- **TFTP-based.** Upgrading firmware by TFTP (Trivial File Transfer Protocol).

- **HTTP-based.** Upgrading firmware by HTTP (HyperText Transfer Protocol).

- **Configuration backup.** The configuration settings of the SMC2582W-B can be backed up to a file via TFTP or HTTP.

- **Configuration reset.** Resetting the configuration settings to factory-default values.

• Management

- **Web-based management** for configuring and monitoring SMC2582W-B via a Web-Browser.
- **SNMP.** SNMP (Simple Network Management Protocol) MIB I, MIB II, IEEE 802.1d, and Private Enterprise MIB are supported.
- **UPnP.** The SMC2582W-B responds to UPnP discovery messages so that a Windows XP user can locate the SMC2582W-B in My Network Places and use a Web browser to configure it.
- **Telnet.** The SMC2582W-B can be managed by Telnet.
- **System log.** For system operational status monitoring.
 - **Local log.** System events are logged to the on-board RAM of the SMC2582W-B and can be viewed using a Web browser.
 - **Remote log by SNMP trap.** Systems events are sent in the form of SNMP traps to a remote SNMP management server.
 - **Remote log by BSD Syslog.** Systems events are sent in the form of BSD Syslog (RFC3164) to a remote Syslog server.
 - **Power over Ethernet (optional).** Supplying power to an SMC2582W-B over an Ethernet cable using SMCPWR-INJ3 Power Injector (IEEE 802.3af compliant). This feature facilitates large-scale wireless LAN deployment.
 - **Hardware Watchdog Timer.** If the firmware gets stuck in an invalid state, the hardware watchdog timer will detect this situation and restart the SMC2582W-B. This way, the SMC2582W-B can provide continuous services.

1.3. LED Definitions

There are several LED indicators on the housing of the SMC2582W-B. They are defined as follows:

- **ALV:** Alive. Blinks when the SMC2582W-B is working normally.
- **RF:** IEEE 802.11b interface activity
- **LAN:** Ethernet LAN interface activity
- **PWR:** Power

2. First-Time Installation and Configuration

2.1. Selecting a Power Supply Method

The SMC2582W-B can be powered by either the supplied power adapter or the optional SMC-PWR-INJ3 EliteConnect™ Power Injector. The SMC2582W-B automatically selects the suitable power depending on your decision.

To power the SMC2582W-B by the supplied power adapter:

1. Plug the power adapter to an AC socket.
2. Plug the connector of the power adapter to the power jack of the SMC2582W-B.

NOTE: This product is intended to be power-supplied by a Listed Power Unit, marked “Class 2” or “LPS” and output rated “5V DC, 1 A minimum” or equivalent statement.

To power the SMC2582W-B by SMC-PWR-INJ3 Power Injector:

1. Connect the power cord cable from power outlet to the SMC-PWR-INJ3 power connector.

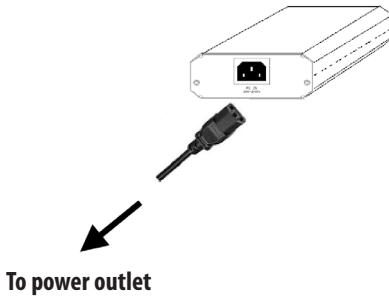


Fig. 1. Connecting the power cord cable to SMC-PWR-INJ3.

2. Check the “POWER” LED: if system is normal, the LED will be on (Green light); otherwise, the “POWER” LED will be off.
3. Connect the Ethernet cable (RJ-45 Category 5) from Ethernet Hub/Switch to the “DATA IN” port of SMC-PWR-INJ3 Power Injector.
4. Connect another Ethernet cable (RJ-45 Category 5) from “POWER & DATA OUT” port of the SMC-PWR-INJ3 Power Injector to the SMC2582W-B Wireless Bridge.

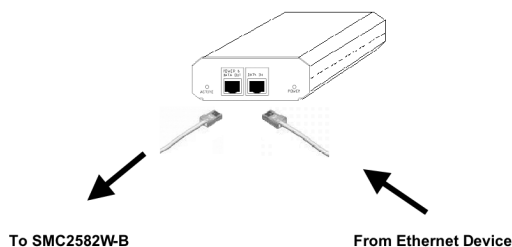


Fig. 2. Connecting Ethernet cables to SMC2582W-B.

5. Check the “ACTIVE” LED: if power is successfully fed into the SMC2582W-B, the “ACTIVE” LED will be on (Red light); otherwise, the “ACTIVE” LED will be off.
6. If the electricity current is over the normal condition ($I_o \div 1.0\text{ A}$), the “ACTIVE” LED will flash (Red light).

NOTE: SMC2582W-B is specially designed for “SMC2582W-B EliteConnect™ 2.4GHz 11Mbps Wireless Bridge. The use of SMC2582W-B with other Ethernet-ready devices that are not compliant to 802.3af may cause damage to the devices.

2.2. Mounting the SMC2582W-B on a Wall

The SMC2582W-B is wall-mountable.

1. Stick the supplied sticker for wall-mounting.
2. Use a $\varnothing 7.0\text{mm}$ drill to drill a 25mm-deep hole at each of the cross marks.
3. Plug in a supplied plastic conical anchor in each hole.
4. Screw a supplied screw in each plastic conical anchor for a proper depth so that the SMC2582W-B can be hung on the screws.
5. Hang the SMC2582W-B on the screws.

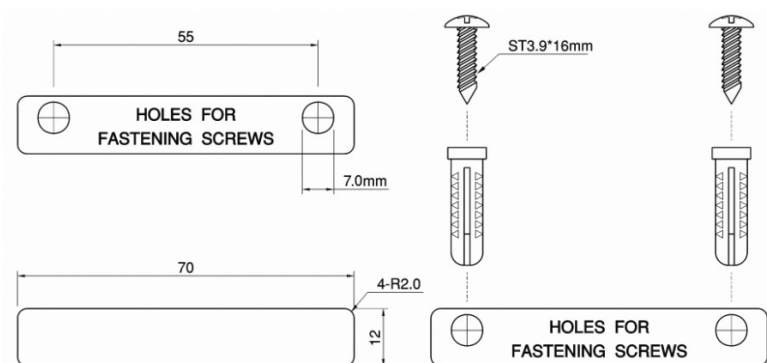


Fig. 3. Mounting the SMC2582W-B on a wall.

2.3. Preparing for Configuration

For you to configure an SMC2582W-B, a managing computer with a Web browser is needed. For first-time configuration of an SMC2582W-B, an Ethernet network interface card (NIC) should have been installed in the managing computer. For maintenance-configuration of a deployed SMC2582W-B, either a wireless computer or a wired computer can be employed as the managing computer.

NOTE: If you are using the browser, Opera, to configure an SMC2582W-B, click the menu item **File**, click **Preferences...**, click **File types**, and edit the MIME type, **text/html**, to add a file extension ".sht" so that Opera can work properly with the Web management pages of the SMC2582W-B.

Since the configuration/management protocol is HTTP-based, you have to make sure that the **IP address of the managing computer and the IP address of the managed SMC2582W-B are in the same IP subnet (the default IP address of an AP is 192.168.2.50 and the default subnet mask is 255.255.255.0.)**

2.3.1. Connecting the Managing Computer and the SMC2582W-B

To connect the Ethernet managing computer and the managed SMC2582W-B for first-time configuration, you have two choices as illustrated in Fig. 4.

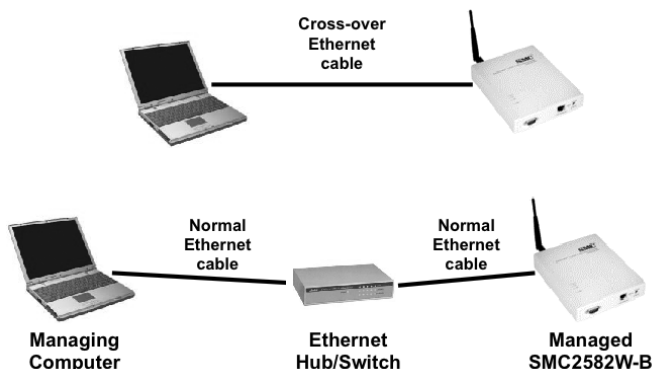


Fig. 4. Connecting a managing computer and an SMC2582W-B via Ethernet.

You can use either a cross-over Ethernet cable (included in the package) or a switch/hub with 2 normal Ethernet cables.

NOTE: One connector of the Ethernet cable must be plugged into the LAN/CONFIG Ethernet jack of the SMC2582W-B for configuration.

2.3.2. Changing the TCP/IP Settings of the Managing Computer

Use the **Windows Network Control Panel Applet** to change the TCP/IP settings of the managing computer, so that the IP address of the computer and the IP address of the SMC2582W-B are in the same IP subnet. Set the IP address of the computer to **192.168.2.xxx** (the default IP address of the SMC2582W-B is **192.168.2.50**) and the subnet mask to **255.255.255.0**.

TIP: You can use **SMC2582W-B Configuration Utility** on the companion CD-ROM to scan for all the SMC2582W-Bs on the network. Double-click a scanned SMC2582W-B to launch the Web browser to manage the SMC2582W-B. Note that this utility does not discover the SMC2682W.

NOTE: On Windows 2000/XP, SMC2582W-B Configuration Utility can only be run by a user with administrator privilege.

NOTE: For some versions of Windows, the computer needs to be restarted for the changes of TCP/IP settings to take effect.

2.4. Configuring the SMC2582W-B

After the IP addressing is configured, launch a Web browser on the managing computer. Then, go to “<http://192.168.2.50>” to access the Start page of the SMC2582W-B’s Web-based management interface.

TIP: For maintenance configuration of an SMC2582W-B, the SMC2582W-B can be reached by its host name using a Web browser. For example, if the SMC2582W-B is named “AP”, you can use the URL “http://AP” to access the Web-based management interface of the SMC2582W-B.

2.4.1. Entering the User Name and Password

Before the start page is shown, you will be prompted to enter the user name and password to gain the right to access the Web-based management interface. For first-time configuration, use the default user name “admin” and default password “smcadmin”, respectively.



Fig. 5. Entering the user name and password.

NOTE: It is strongly recommended that the password be changed to other value for security reasons. On the start page, click the **General, Password** link to change the value of the password (see Section 3.3.1 for more information).

TIP: Since the start page shows the current settings and status of the SMC2582W-B, it can be saved or printed within the Web browser for future reference.

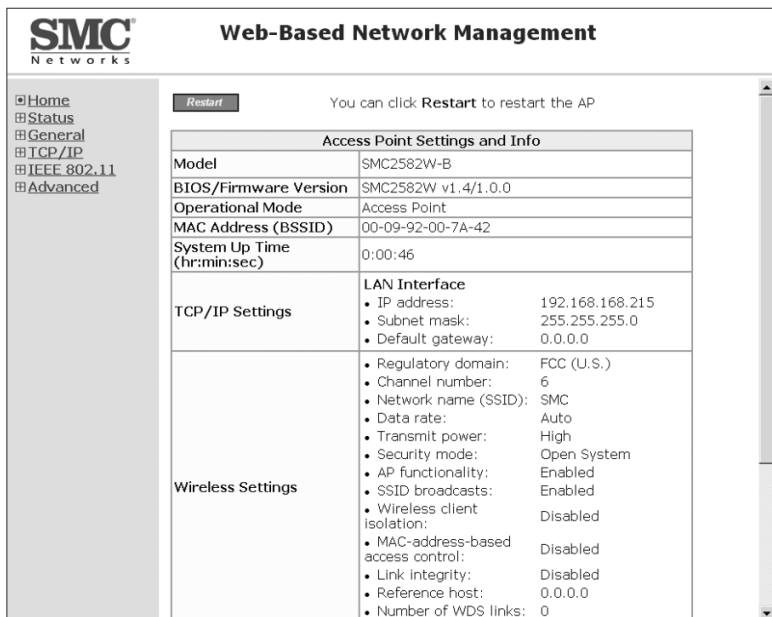


Fig. 6. The Start page.

2.4.2. Step 1: Selecting an Operational Mode

Access Point / Bridge

Use this mode to provide both Access Point and Bridging Functionality. The Bridge function is supported through Wireless Distribution System (WDS). The WDS function can support up to 6 bridge links.

Bridge Master and Bridge Slave

These 2 modes can be used when you want to use both the SMC2682W and SMC2582W-B in the same bridging environments. If you are setting up a bridge configuration using all SMC2582W-B's use the [Access Point / Bridge] mode above and configure your Bridge connections using WDS.

Bridge Master

Use this mode to provide the Master Bridge functionality of the SMC2682W. In this mode, the SMC2582W-B can also act as an Access Point to the wireless clients located on the same network as the Bridge Master.

Bridge Slave

Use this mode to provide Slave Bridge functionality of the SMC2682W, in this mode the SMC2582W-B will not work as an Access Point.

Fig. 7. Operational modes settings.

The SMC2582W-B supports 3 operational modes for meeting various wireless connectivity requirements:

- **Access Point (AP).** The AP mode enables IEEE 802.11 Stations (STAs) to automatically associate with it via the standard IEEE 802.11 association process. In addition, the IEEE 802.11 WDS (Wireless Distribution System) technology can be used to manually establish wireless links between two APs or between an AP and a Bridge Master.
- **Bridge Master (BM).** Use this mode to provide the Bridge Master functionality of the SMC2682W. The Bridge Master mode is designed to work in those networks where SMC2682W Wireless Bridge Slaves are already installed. The Bridge Master enables Bridge Slaves to automatically associate with it. It also enables IEEE 802.11 Stations, which are on the same LAN as the Bridge Master, to automatically associate with it via the standard IEEE 802.11 association process. In addition, the IEEE 802.11 WDS (Wireless Distribution System) technology can be used to manually establish wireless links between two Bridge Masters or between a Bridge Master and an AP.
- **Bridge Slave (BS).** Use this mode to provide the Bridge Slave functionality of the SMC2682W. The Bridge Slave mode is designed to work in those networks where SMC2682W Wireless Bridge Masters are already installed.

In any mode, the SMC2582W-B forwards packets between its Ethernet interface and wireless interface for wired hosts on the Ethernet side and wireless host(s) on the wireless side.

There are 2 types of wireless links between two SMC2582W-Bs or between an SMC2582W-B and another wireless device.

- **WDS.** This type of wireless link is specified in the IEEE 802.11 standard for communication between two IEEE 802.11 APs. Wireless packets transmitted along the WDS link comply with the IEEE 802.11 WDS (Wireless Distribution System) format at the link layer.
- **BM-BS.** This type of wireless link is used in the SMC2682W for providing LAN-to-LAN bridging services. To establish this type of wireless link between two SMC2682W, one SMC2682W must be in Bridge Master (BM) mode and the other must be in Bridge Slave (BS) mode. The SMC2582W-B provides this type of wireless link for backward compatibility with the SMC2682W. The relationships among the operational modes and the wireless link types are shown in the following table:

Table 1. Operational modes vs. wireless link types.

	AP	BM	BS
AP	WDS	WDS	
BM	WDS	WDS	BM-BS
BS		BM-BS	

From the table, a WDS link can be established between two APs, a BM-BS link can be established between a Bridge Master and a Bridge Slave, but no wireless link can be established between a Bridge Slave and an AP.

Select an operational mode and click **Save** at the bottom of this page, and then you are brought back to the start page.

2.4.3. Step 2: Configuring TCP/IP Settings

Method of obtaining an IP address:	<input type="text" value="Set Manually"/>
IP address:	<input type="text" value="192.168.168.214"/>
Subnet mask:	<input type="text" value="255.255.255.0"/>
Default gateway:	<input type="text" value="0.0.0.0"/>
Host name:	<input type="text" value="AP1"/>
Domain (DNS suffix):	<input type="text"/>

Fig. 8. TCP/IP settings.

Go to the **TCP/IP Addressing** section to configure IP address settings. The IP address can be manually set or automatically assigned by a DHCP server on the LAN. If you are manually setting the **IP address**, **Subnet mask**, and **Default gateway** settings, set them appropriately, so that they comply with your LAN environment. In addition, you can specify the **Host name** and **Domain (DNS suffix)** of the SMC2582W-B.

When you are finished, click **Save** at the bottom of this page, and then you are brought back to the start page.

2.4.4. Step 3: Configuring IEEE 802.11 Settings

AP functionality:	<input type="text" value="Enabled"/>
Regulatory domain:	<input type="text" value="FCC (U.S.)"/>
Channel number:	<input type="text" value="6"/>
Network name (SSID):	<input type="text" value="SMC"/>

Fig. 9. IEEE 802.11b communication settings.

Go to the **IEEE 802.11, Communication** section to configure IEEE 802.11b-related communication settings, including **Channel number** and **Network name (SSID)**.

The number of available RF channels depends on local regulations.

NOTE: The **Regulatory domain** setting of the SMC2582W-B sold in the U.S. and Canada is not configurable. It is set to FCC by default. As a result, only channels from 1 to 11 are available.

NOTE: For two SMC2582W-Bs or one wireless client computer and one SMC2582W-B to establish a wireless link, both devices must be configured with the same channel number and SSID.

If the SMC2582W-B was configured to be in AP or Bridge Master mode, and you want to use WDS to establish inter-SMC2582W-B wireless links, configure the WDS settings.

Port	Enabled	Peer MAC Address
1	<input type="checkbox"/>	00-02-6F-01-62-C5
2	<input type="checkbox"/>	
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	
6	<input type="checkbox"/>	

Fig. 10. Wireless Distribution System settings.

To enable a WDS link:

- 1. Specify the MAC address of the AP or bridge at the other end of the WDS link.
- 2. Select the corresponding Enabled check box.

For example, assume you want two SMC2582W-Bs with MAC addresses 00-02-65-01-62-C5 and 00-02-65-01-62-C6 to establish a WDS link between them. On SMC2582W-B 00-02-65-01-62-C5, set the peer MAC address of port 1 to 00-02-65-01-62-C6 and on SMC2582W-B 00-02-65-01-62-C6, set the peer MAC address of port 1 to 00-02-65-01-C5.

TIP: Plan your wireless network and draw a diagram, so that you know how the SMC2582W-B is connected to other peer APs or wireless bridges by WDS.

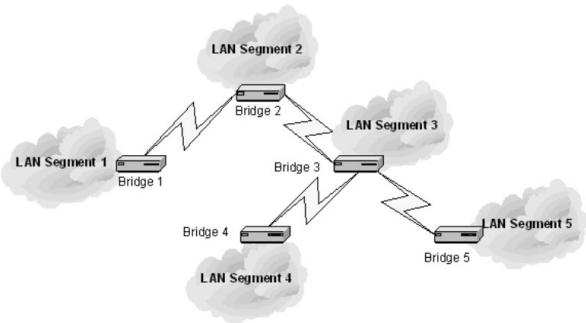


Fig. 11. Sample wireless bridge network topology.

WARNING: Don't let your network topology consisting of wireless bridges, Ethernet switches, Ethernet links, and WDS links contain loops. If any loops exist, packets will circle around the loops and network performance will be seriously degraded.

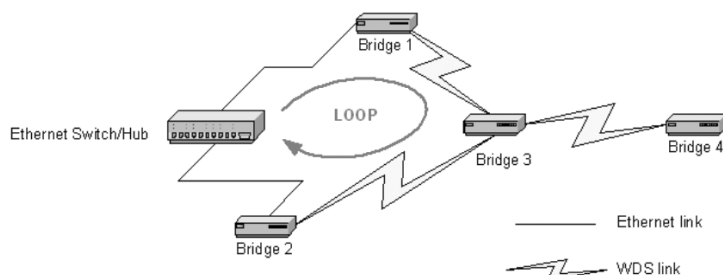


Fig. 12. Network topology containing a loop.

When you are finished, click **Save** at the bottom of this page, and then you are brought back to the start page.

2.4.5. Step 4: Reviewing and Applying Settings

Restart
Cancel

The settings have been changed. Click **Restart** to restart the access point for the settings to take effect.

Access Point Settings and Info	
Model	SMC2582W-B
BIOS/Firmware Version	SMC2582W v1.4/1.0.0
Operational Mode	Access Point
MAC Address (BSSID)	00-09-92-00-7A-42
System Up Time (hr:min:sec)	0:11:20
TCP/IP Settings	LAN Interface <ul style="list-style-type: none"> IP address: 192.168.168.201 Subnet mask: 255.255.255.0 Default gateway: 192.168.168.1
	<ul style="list-style-type: none"> Regulatory domain: FCC (U.S.) Channel number: 11 Network name (SSID): SMC Data rate: Auto Transmit power: High

Fig. 13. Settings changes are highlighted in red.

On the start page, you can review all the settings you have made. Changes are highlighted in red. If they are ok, click **Restart** to restart the SMC2582W-B for the new settings to take effect.

NOTE: About 7 seconds are needed for the SMC2582W-B to complete its restart process.

2.5. Deploying the SMC2582W-B

After the settings have been configured, deploy the SMC2582W-B to the field application environment. Connect the SMC2582W-B to an Ethernet LAN through an Ethernet switch/hub.

If external high-gain directional antennas are used for a long-range wireless bridging application, it may be difficult to align the antennas. Here is a suggestion for antenna alignment.

To adjust the alignments of a pair of SMC high-gain antennas:

1. Connect each SMC2582W-B to a computer via Ethernet.
2. Configure the data rate of each SMC2582W-B to the lowest value, 1Mbps.
3. Fix the alignment of the antenna on one side.
4. Adjust the alignment of the antenna on other side by using response time information obtained from PINGing (run PING.exe) the “fixed-side” computer.
5. Fine-tune the alignment of the antenna until you get a best response time.
6. Increase the data rate of each SMC2582W-B simultaneously until a maximal workable data rate is reached. You may not be able to use the highest data rate, 11Mbps, because of the distance and the gain of the antennas.

Fig. 14 illustrates the idea.

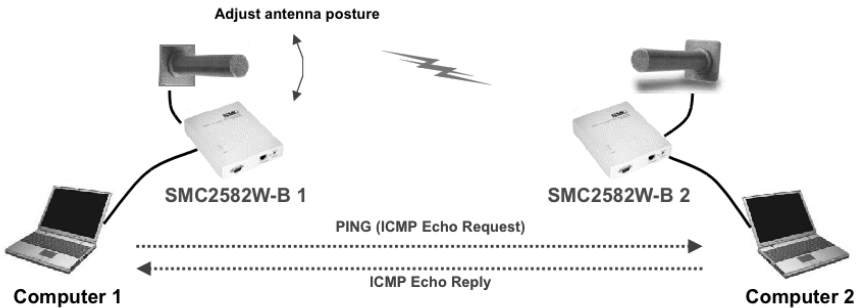


Fig. 14. Adjusting alignments of external directional antennas.

3. Using Web-Based Management

In this chapter, we'll explain each Web management page of the SMC2582W-B.

3.1. Overview

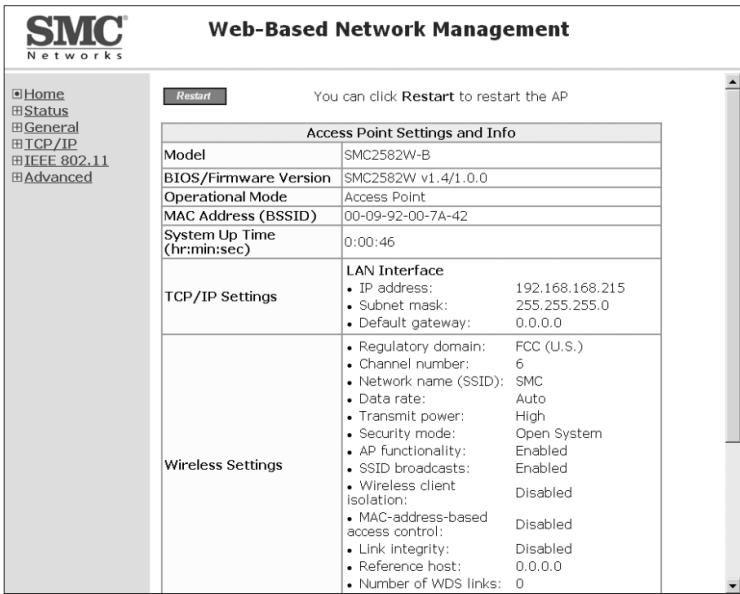


Fig. 15. The Start page.

3.1.1. Menu Structure

The left side of the start page contains a menu for you to carry out commands. Here is a brief description of the hyperlinks on the menu:

- **Home.** For going back to the start page.
- **Status.** Status information.
 - **Wireless Clients.** The status of the wireless clients (STAs and Bridge Slaves) currently associated with the SMC2582W-B.
 - **DHCP Mappings.** Current IP-MAC address mappings of the built-in DHCP server.

- **System Log.** System events log.
- **General.** Global operations.
 - **Operational Mode.** Operational mode settings.
 - **Password.** For gaining rights to change the settings of the SMC2582W-B.
 - **Firmware Tools.** For upgrading the firmware of the SMC2582W-B, backing up and restoring configuration, and configuration reset settings of the SMC2582W-B.
- **TCP/IP.** TCP/IP- related settings.
 - **Addressing.** IP address settings for the SMC2582W-B to work with TCP/IP.
 - **DHCP Server.** Settings for the DHCP (Dynamic Host Configuration Protocol) server on the SMC2582W-B.
- **IEEE 802.11.** IEEE 802.11b-related settings.
 - **Communication.** Basic settings for the IEEE 802.11b interface of the SMC2582W-B to work properly with wireless clients.
 - **Security.** Security settings for authenticating wireless users and encrypting wireless data.
- **Advanced.** Advanced settings of the SMC2582W-B.
 - **Packet Filters.** Ethernet Type Filters, IP Protocol Filters, and TCP/UDP Port Filters settings.
 - **Management.** UPnP, System Log, and SNMP settings.

3.1.2. Save, Save & Restart, and Cancel Commands



Fig. 16. Save, Save & Restart, and Cancel.

At the bottom of each page that contains settings you can configure, there are up to three buttons—**Save**, **Save & Restart**, and **Cancel**. Clicking **Save** stores the settings changes to the memory of the SMC2582W-B and brings you back to the start page. Clicking **Save & Restart** stores the settings changes to the memory of the SMC2582W-B and restarts the SMC2582W-B immediately for the settings to take effect. Clicking **Cancel** discards any settings changes and brings you back to the start page.

If you click **Save**, the start page will reflect the fact that the configuration settings have been changed by showing two buttons—**Restart** and **Cancel**. In addition, changes are highlighted in red. Clicking **Cancel** discards all the changes. Clicking **Restart** restarts the SMC2582W-B for the settings to take effect.

[Restart](#)
[Cancel](#)

The settings have been changed. Click **Restart** to restart the access point for the settings to take effect.

Access Point Settings and Info	
Model	SMC2582W-B
BIOS/Firmware Version	SMC2582W v1.4/1.0.0
Operational Mode	Access Point
MAC Address (BSSID)	00-09-92-00-7A-42
System Up Time (hr:min:sec)	0:11:20
TCP/IP Settings	LAN Interface <ul style="list-style-type: none"> IP address: 192.168.168.201 Subnet mask: 255.255.255.0 Default gateway: 192.168.168.1
	<ul style="list-style-type: none"> Regulatory domain: FCC (U.S.) Channel number: 11 Network name (SSID): SMC Data rate: Auto Transmit power: High

Fig. 17. Settings have been changed.

3.1.3. Home and Refresh Commands



Fig. 18. Home and Refresh.

At the bottom of each status page that shows read-only information, there are two buttons—**Home** and **Refresh**. Clicking **Home** brings you back to the start page. Clicking **Refresh** updates the shown status information.

3.2. Viewing Status

3.2.1. Associated Wireless Clients

Wireless Clients Status						
No.	MAC Address	IP Address	Name	Tx Bytes	Rx Bytes	Last Activity Time
1	00-90-48-00-40-94	192.168.168.226		7521	1162	00h:01m:56s

Fig. 19. Status of associated wireless clients.

On this page, the status information of each associated client (STA or Bridge Slave), including its MAC address, IP address, user name, number of bytes it has send, number of bytes it has received, and the time of its last activity, is shown.

3.2.2. Current DHCP Mappings

DHCP Mapping Table			
No.	MAC Address	IP Address	Type
1	00-90-4B-00-B9-BD	192.168.168.214	Static
2	00-BB-DE-AD-BE-EF	192.168.168.224	In use
3	00-90-4B-00-40-94	192.168.168.226	Dynamic
4	00-40-01-43-1D-E8	192.168.168.230	In use

Fig. 20 Current DHCP mappings.

On this page, all the current static or dynamic DHCP mappings are shown. A DHCP mapping is a correspondence relationship between an IP address assigned by the DHCP server and a computer or device that obtains the IP address. A computer or device that acts as a DHCP client is identified by its MAC address.

A static mapping indicates that the DHCP client always obtains the specified IP address from the **DHCP server**. You can set static DHCP mappings in the **Static DHCP Mappings** section of the DHCP Server configuration page (see Section 3.4.2). A dynamic mapping indicates that the DHCP server chooses an IP address from the IP address pool from the **DHCP Server** configuration page.

3.2.3. System Log

Model:	SMC2582W-B
BIOS/Firmware version:	SMC2582W v1.4/2.5.3.4084
Operational mode:	Access Point
Current time:	08/07/2003 14:30:40
08/07/2003 14:18:46 SYSTEM START UP!	
08/07/2003 14:18:46 Wireless LAN interface initializes success.	
08/07/2003 14:18:46 BSSID --> 00-02-6F-01-67-CC	
08/07/2003 14:18:46 LAN IP address --> 192.168.168.218.	
08/07/2003 14:18:55 The administrator from 192.168.168.139 logs in the device successfully.	
08/07/2003 14:30:29 The administrator from 192.168.168.220 logs in the device successfully.	

Fig. 21. System log.

System events are recorded in the memory of the SMC2582W-B. The logged information is useful for troubleshooting purposes. The system events are divided into several categories, and you can select which categories of events to log. See Section 3.6.2.3 for more information.

3.3. General Operations

3.3.1. Selecting an Operational Mode

- ⑥ **Access Point / Bridge**
Use this mode to provide both Access Point and Bridging Functionality. The Bridge function is supported through Wireless Distribution System (WDS). The WDS function can support up to 6 bridge links.

Bridge Master and Bridge Slave
These 2 modes can be used when you want to use both the SMC2682W and SMC2582W-B in the same bridging environments. If you are setting up a bridge configuration using all SMC2582W-B's use the [Access Point / Bridge] mode above and configure your Bridge connections using WDS.

○ **Bridge Master**
Use this mode to provide the Master Bridge functionality of the SMC2682W. In this mode, the SMC2582W-B can also act as an Access Point to the wireless clients located on the same network as the Bridge Master.

○ **Bridge Slave**
Use this mode to provide Slave Bridge functionality of the SMC2682W, in this mode the SMC2582W-B will not work as an Access Point.

Fig. 22. Operational modes settings.

The SMC2582W-B supports 3 operational modes for meeting various wireless connectivity requirements:

- **Access Point (AP).** The AP mode enables IEEE 802.11 Stations (STAs) to automatically associate with it via the standard IEEE 802.11 association process. In addition, the IEEE 802.11 WDS (Wireless Distribution System) technology can be used to manually establish wireless links between two APs or between an AP and a Bridge Master.
- **Bridge Master (BM).** Use this mode to provide the Bridge Master functionality of the SMC2682W. The Bridge Master mode is designed to work in those networks where SMC2682W Wireless Bridge Slaves are already installed. The Bridge Master enables Bridge Slaves to automatically associate with it. It also enables IEEE 802.11 Stations, which are on the same LAN as the Bridge Master, to automatically associate with it via the standard IEEE 802.11 association process. In addition, the IEEE 802.11 WDS (Wireless Distribution System) technology can be used to manually establish wireless links between two Bridge Masters or between a Bridge Master and an AP.
- **Bridge Slave (BS).** Use this mode to provide the Bridge Slave functionality of the SMC2682W. The Bridge Slave mode is designed to work in those networks where SMC2682W Wireless Bridge Masters are already installed.

In any mode, the SMC2582W-B forwards packets between its Ethernet interface and wireless interface for wired hosts on the Ethernet side and wireless host(s) on the wireless side.

There are 3 types of wireless links between two SMC2582W-Bs or between an SMC2582W-B and another wireless device.

- **STA-AP.** This type of wireless link is specified in the IEEE 802.11 standard for communication

between an IEEE 802.11 Station (STA) and an IEEE 802.11 Access Point (AP). An STA is usually a client computer (PC or PDA) with a WLAN network interface card (NIC).

- **WDS.** This type of wireless link is specified in the IEEE 802.11 standard for communication between two IEEE 802.11 APs. Wireless packets transmitted along the WDS link comply with the IEEE 802.11 WDS (Wireless Distribution System) format at the link layer.
- **BM-BS.** This type of wireless link is propriety and was used in the legacy SMC2682W for providing LAN-to-LAN bridging services. To establish this type of wireless link between two SMC2682W, one SMC2682W must be in Bridge Master (BM) mode and the other must be in Bridge Slave (BS) mode. The SMC2582W-B provides this type of wireless link for backward compatibility with the SMC2682W.

The relationships among the operational modes and the wireless link types are shown in the following table:

	AP	BM	BS
AP	WDS	WDS	
BM	WDS	WDS	BM-BS
BS		BM-BS	

Table 2. Operational modes vs. wireless link types.

From the table, a WDS link can be establish between two APs, a BM-BS link can be established between a Bridge Master and a Bridge Slave, but no wireless link can be established between a Bridge Slave and an AP.

3.3.2. Changing Password

Old password:	<input type="password"/>
New user name:	<input type="text" value="admin"/>
New password:	<input type="password"/>
New password again:	<input type="password"/>

Fig. 23. Password.

On this page, you can change the user name and password for the right to modify the configuration of the SMC2582W-B. The new password must be typed twice for confirmation.

3.3.3. Managing Firmware

Firmware management protocol:	<input type="text" value="HTTP"/>
-------------------------------	-----------------------------------

Fig. 24. Firmware management protocol setting.

Firmware management operations for the SMC2582W-B include **firmware upgrade**, **configuration backup**, **configuration restore**, and configuration **reset**. Firmware upgrade, configuration

backup, and configuration restore can be achieved via HTTP or TFTP. The HTTP-based way is suggested because it's more user-friendly. However, due to different behavior of different Web browser types and versions, HTTP-based firmware management operations may not work properly with some Web browsers. If you cannot successfully perform HTTP-based firmware management operations with your Web browser, try the TFTP-based method.

3.3.3.1. Upgrading Firmware by HTTP

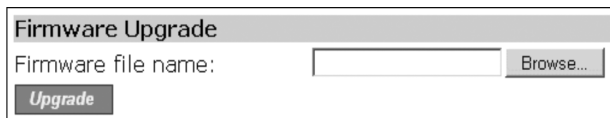


Fig. 25. Firmware upgrade by HTTP.

To upgrade firmware of the SMC2582W-B by HTTP:

1. Click **Browse** and then select a correct firmware .bin file. The firmware file path will be shown in the **Firmware file name** text box.
2. Click **Upgrade** to begin the upgrade process.

3.3.3.2. Backing up and Restoring Configuration Settings by HTTP

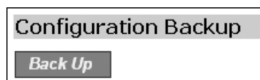


Fig. 26. Firmware backup by HTTP.

To back up configuration of the SMC2582W-B by HTTP:

1. Click **Back Up**.
2. You'll be prompted to open or save the configuration file. Click Save.
3. The configuration file is named by the SMC2582W-B's MAC address. For example, if the SMC2582W-B's MAC address is 00-01-02-33-44-55, the configuration backup file should be "000102334455.hex". Don't change the configuration file name in the Save As dialog box. Select a folder in which the configuration file is to be stored. And then, click Save.

NOTE: The procedure may be a little different with different Web browsers.

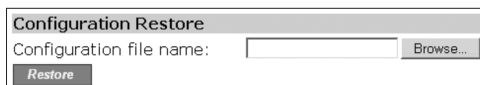


Fig. 27. Configuration restore by HTTP.

To restore configuration of the SMC2582W-B by HTTP:

1. Click **Browse** and then select a correct configuration **.hex** file. You have to make sure the file name is the SMC2582W-B's MAC address. The firmware file path will be shown in the **Firmware file name** text box.
2. Click **Restore** to upload the configuration file to the SMC2582W-B.

3.3.3.3. Upgrading Firmware by TFTP

TFTP server IP address:	<input type="text" value="192.168.0.19"/>
Max number of retries:	<input type="text" value="30"/>
Timeout:	<input type="text" value="10 sec."/>

Fig. 28. TFTP server settings.

When use TFTP as the firmware management protocol, you can configure settings for the SMC2582W-B's TFTP client to communicate with a TFTP server. If the TFTP client does not get a response from the TFTP server within a period specified by the **Timeout** setting, it will resend the previous request. **The Max number of retries** setting specifies the maximal number of resend before the TFTP client stops communicating with the TFTP server.

The SMC2582W-B Installation CD includes a TFTP server program (TftpSrvr.exe) for firmware upgrade. Run this program on the computer that serves as a TFTP server.



Fig. 29. Firmware upgrade by TFTP.

To upgrade firmware of the SMC2582W-B by TFTP:

1. Get a computer that will be used as a TFTP server and as a managing computer to trigger the upgrade process.
2. Connect the computer and one of the LAN Ethernet switch port with a normal Ethernet cable.
3. Configure IP address of the computer so that the SMC2582W-B and the computer are in the same IP subnet.
4. On the computer, run the TFTP Server utility. And specify the folder in which the firmware files reside.
5. On the computer, run a Web browser and click the General, Firmware Tools hyperlink.
6. Choose TFTP as the Firmware management protocol.
7. Specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type IpConfig, then press the **Enter** key.
8. Trigger the firmware upgrade process by clicking **Upgrade**.



Fig. 30. TFTP Server.

NOTE: After the dialog box of the TFTP server program appears, be sure to specify the working folder within which the downloaded firmware files reside.

NOTE: Make sure the Accept read requests check box of TFTP Server is selected.

NOTE: The LAN IP address of the SMC2582W-B and the IP address of the TFTP server must be in the same IP subnet for TFTP to work.

NOTE: It is highly recommended that the TFTP server and the to-be-upgraded SMC2582W-B be connected by Ethernet and on the same LAN.

NOTE: After the firmware is upgraded, be sure to delete the contents of the Web browser cache, so that the Web management pages can be shown correctly.

NOTE: A failed upgrade may corrupt the firmware and make the SMC2582W-B unstartable. When this occurs, call for technical support.

TIP: If you want to remotely upgrade the firmware of a deployed SMC2582W-B from the Internet, adjust the Timeout and Max no. of retries settings of TFTP Server for remote TFTP upgrade to succeed.

3.3.3.4. Backing up and Restoring Configuration Settings by TFTP



Fig. 31. Configuration backup/restore.

To back up configuration of the SMC2582W-B by TFTP:

1. Get a computer that will be used as a TFTP server and as a managing computer to trigger the backup process.
2. Connect the computer and one of the LAN Ethernet switch port with a normal Ethernet cable.
3. Configure the IP address of the computer so that the computer and the SMC2582W-B are in the same IP subnet.
4. On the computer, run the TFTP Server utility. Select the **Accept write requests** check box, and specify the folder to which the configuration settings of the SMC2582W-B will be saved.
5. On the computer, run a Web browser and click the **General, Firmware Tools** hyperlink.
6. Choose **TFTP** as the **Firmware management protocol**.
7. Within the **Configuration Backup/Restore** section, specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type IpConfig, then press the **Enter** key.
8. Trigger the backup process by clicking **Back Up**. The SMC2582W-B's configuration settings will be saved as "**AaBbCcDdEeFf.hex**" by the TFTP server, where "AaBbCcDdEeFf" is the SMC2582W-B's MAC address. For example, if the SMC2582W-B's MAC address is 00-01-02-33-44-55, the configuration backup file will be "000102334455.hex".

NOTE: Remember to select the **Accept write requests** check box of TFTP Server.

To restore configuration of the SMC2582W-B by TFTP:

1. Get a computer that will be used as a TFTP server and as a managing computer to trigger the restoring process.
2. Connect the computer and one of the LAN Ethernet switch port with a normal Ethernet cable.
3. Configure the IP address of the computer so that the computer and the SMC2582W-B are in the same IP subnet.
4. On the computer, run the TFTP Server utility. And specify the folder in which the configuration backup file resides. A configuration backup file is named by the SMC2582W-B's MAC address. For example, if the SMC2582W-B's MAC address is 00-01-02-33-44-55, the configuration backup file should be "000102334455.hex".
5. On the computer, run a Web browser and click the **General, Firmware Tools** hyperlink.
6. Choose **TFTP** as the **Firmware management protocol**.
7. Within the **Configuration Backup/Restore** section, specify the IP address of the computer, which acts as a TFTP server. If you don't know the IP address of the computer, open a Command Prompt, and type IpConfig, then press the **Enter** key.
8. Trigger the restoring process by clicking **Restore**. The SMC2582W-B will then download the configuration backup file from the TFTP server.

NOTE: Make sure the file is a valid configuration backup file for the SMC2582W-B.

TIP: If you want to remotely back up or restore configuration from the Internet, adjust the **Timeout** and **Max no. of retries** settings of TFTP Server for remote TFTP configuration backup/restore to succeed.

3.3.3.5. Resetting Configuration to Factory Defaults

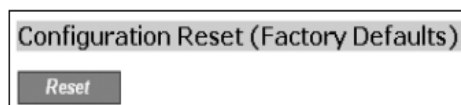


Fig. 32. Configuration reset.

Clicking the Reset button resets the device configuration to factory defaults.

WARNING: Think twice before clicking the Reset button. You'll lose all your current configuration settings.

3.4. Configuring TCP/IP Related Settings

3.4.1. Addressing

Method of obtaining an IP address:	<input type="text" value="Set Manually"/>
IP address:	<input type="text" value="192.168.168.214"/>
Subnet mask:	<input type="text" value="255.255.255.0"/>
Default gateway:	<input type="text" value="0.0.0.0"/>
Host name:	<input type="text" value="AP1"/>
Domain (DNS suffix):	<input type="text"/>

Fig. 33. TCP/IP settings.

The IP address of the SMC2582W-B can be manually set (**Set Manually**) or automatically assigned by a DHCP server on the LAN (**Obtain from a DHCP Server**). If you are manually setting the IP **address**, **Subnet mask**, and **Default gateway** settings, set them appropriately, so that they comply with your LAN environment. In addition, you can specify the **Host name** and **Domain (DNS suffix)** of the SMC2582W-B.

3.4.2. DHCP Server

3.4.2.1. Basic

Functionality:	Enabled
Default gateway:	192.168.2.1
Subnet mask:	255.255.255.0
Primary DNS server:	192.168.2.1
Secondary DNS server:	
First allocatable IP address:	192.168.2.2
Allocatable IP address count:	20

Fig. 34. Basic DHCP server settings.

The SMC2582W-B can automatically assign IP addresses to client computers by DHCP. In this section of the management page, you can specify the **Default gateway**, **Subnet mask**, **Primary DNS server**, and **Secondary DNS** server settings that will be sent to a client at its request. Additionally, you can specify the first IP address that will be assigned to the clients and the number of allocatable IP addresses.

NOTE: There should be only one DHCP server on the LAN; otherwise, DHCP would not work properly. If there is already a DHCP server on the LAN, disable the DHCP server functionality of the SMC2582W-B.

NOTE: By default the DHCP server function is disabled.

3.4.2.2. Static DHCP Mappings

Enabled	Desc.	MAC Address	IP Address
<input type="checkbox"/>	Bill	00-22-32-5D-80-02	192.168.0.203
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			

Fig. 35. Static DHCP mappings.

IP addresses of servers are often static so that clients could always locate the servers by the static IP addresses. By **Static DHCP Mappings**, you can ensure that a host will get the same IP address when it requests one from the DHCP server. Therefore, instead of configuring the IP address of an intranet server manually, you can configure the server to obtain an IP address by DHCP and it is

always assigned the same IP address.

To always assign a static IP address to a specific DHCP client:

1. Specify the MAC address of the DHCP client and the IP address to be assigned to it. Then, give a description of this mapping.
2. Select the corresponding **Enabled** check box.

3.5. Configuring IEEE 802.11b-Related Settings

3.5.1. Communication

3.5.1.1. Basic

Basic IEEE 802.11b-related communication settings include **AP functionality**, **Channel number**, **Network name (SSID)**, **Data rate**, and **Transmit power**.

AP functionality:	Enabled
Regulatory domain:	FCC (U.S.)
Channel number:	6
Network name (SSID):	SMC
Data rate:	Auto
Transmit power:	High

Fig. 36. Basic IEEE 802.11b communication settings.

For specific needs such as configuring the SMC2582W-B as a wireless LAN-to-LAN bridge, the AP functionality can be disabled, so that no wireless client can associate with the SMC2582W-B.

The number of available RF channels depends on local regulations; therefore you have to choose an appropriate regulatory domain to comply with local regulations. The SSID of a wireless client computer and the SSID of the SMC2582W-B must be identical for them to communicate with each other.

NOTE: The **Regulatory domain** setting of the SMC2582W-B sold in the U.S. and Canada is not configurable. It is set to FCC by default. As a result, only channels from 1 to 11 are available.

If there is RF interference, you may want to reduce the **Data rate** for more reliable wireless transmission. In most cases, leave the setting to **Auto**.

The transmit power of the RF module of the SMC2582W-B can be adjusted so that the RF coverage of the SMC2582W-B can be changed.

3.5.1.2. Link Integrity

Functionality:	Disabled
Reference host:	0.0.0.0

Fig. 37. Link integrity settings.

When the SMC2582W-B is in AP or Bridge Master mode and the Ethernet LAN interface is detected to be disconnected from the wired network, all currently associated wireless clients (STAs and Bridge Slaves) are disassociated by the SMC2582W-B and no wireless client can associate with the SMC2582W-B. The detection mechanism is based on pinging the IP address specified in **Reference host**.

3.5.1.3. Wireless Distribution System

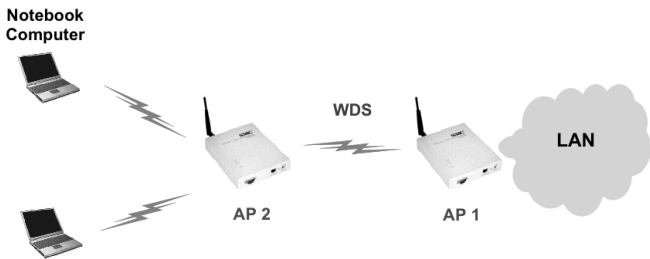


Fig. 38. Wireless Distribution System.

Traditionally, access points are connected by Ethernet. By IEEE 802.11 Wireless Distribution System (WDS), APs can communicate with one another wirelessly. For example, in Fig. 38, AP 2 acts as an access point for the notebook computers and it forwards packets sent from the notebook computers to AP 1 through WDS. Then, AP 1 forwards the packets to the Ethernet LAN. Packets destined for the notebook computers follow a reverse path from the Ethernet LAN through the APs to the notebook computers. In this way, AP 2 plays a role of “AP repeater”.



Fig. 39. LAN-to-LAN bridging.

By WDS, two or more LAN segments can be connected wirelessly. As illustrated in Fig. 39, a pair of wireless LAN-to-LAN bridges is used to connect two LAN segments. Since the SMC2582W-B is WDS-enabled, it can be used as a wireless bridge even when it is in AP mode.

NOTE: An SMC2582W-B can have up to 6 WDS links to other APs or wireless bridges.

Port	Enabled	Peer MAC Address
1	<input type="checkbox"/>	00-02-6F-01-62-C5
2	<input type="checkbox"/>	
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	
6	<input type="checkbox"/>	

Fig. 40. Wireless Distribution System settings.

To enable a WDS link:

3. Specify the MAC address of the AP or bridge at the other end of the WDS link.
4. Select the corresponding Enabled check box.

For example, assume you want two SMC2582W-Bs with MAC addresses 00-02-65-01-62-C5 and 00-02-65-01-62-C6 to establish a WDS link between them. On SMC2582W-B 00-02-65-01-62-C5, set the peer MAC address of port 1 to 00-02-65-01-62-C6 and on SMC2582W-B 00-02-65-01-62-C6, set the peer MAC address of port 1 to 00-02-65-01-C5.

TIP: Plan your wireless network and draw a diagram, so that you know how an AP is connected to other peer APs or wireless bridges by WDS.

TIP: Plan your wireless network and draw a diagram, so that you know how a bridge is connected to other peer bridges by WDS. See the following figure for an example network-planning diagram.

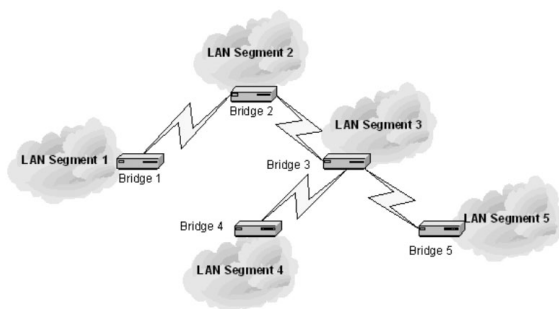


Fig. 41. Sample wireless bridge network topology.

WARNING: Don't let your network topology consisting of wireless bridges, Ethernet switches, Ethernet links, and WDS links contain loops. If any loops exist, packets will circle around the loops and network performance will be seriously degraded.

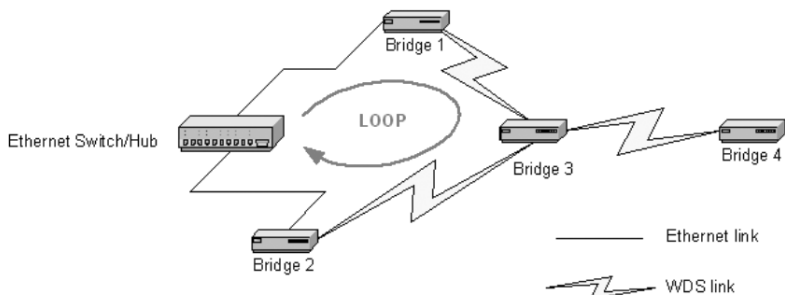


Fig. 42. Network topology containing a loop.

3.5.2. Security

IEEE 802.11b security settings include **SSID broadcasts**, **Wireless client isolation**, **Security mode**, **IEEE 802.11 Authentication algorithm**, **WEP keys**, **MAC-Address-Based Access Control**.

3.5.2.1. Basic

SSID broadcasts:	Enabled
Wireless client isolation:	Disabled
Security mode:	Static WEP
Authentication algorithm:	Auto
Key length:	64 Bits
Selected key:	Key 1
Key 1:	*****
Key 2:	*****
Key 3:	*****
Key 4:	*****

Fig. 43. Basic IEEE 802.11b security settings.

For security reasons, it is highly recommended that the security mode be set to options other than Open System. When the security mode is set to Open System, no authentication and data encryption will be performed. Additionally, you can disable the SSID broadcasts functionality so that a wireless client (STA or Bridge Slave) with an "any" SSID cannot associate with the SMC2582W-B.

Wireless Client Isolation is a feature for the SMC2582W-B in AP or Bridge Master mode to block wireless-to-wireless traffic between STAs so that the STAs cannot see each other. This feature is useful for WLANs deployed in public places. In this way, hackers have no chance to attack other wireless users in a hotspot.

When the **Wireless client isolation** setting is set to **This AP Only**, wireless clients (STAs) of this SMC2582W-B as an AP cannot see each other, and wireless-to-wireless traffic between the STAs is blocked. When the setting is set to **All APs in This Subnet**, traffic among wireless users of different

SMC2582-Bs in the same IP subnet is blocked. The behaviors are illustrated in the following figures.

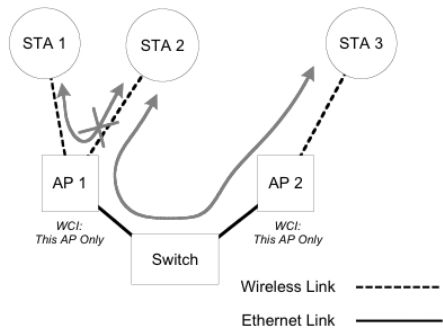


Fig. 44. Behavior of the “This AP Only” wireless client isolation option.

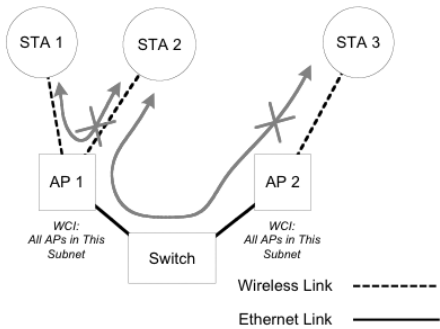


Fig. 45. Behavior of the “All APs on This Subnet” wireless client isolation option.

As illustrated in Fig 44 when AP 1 and AP 2 are using the “This AP Only” option, wireless traffic between STA 1 and STA 2 is blocked by AP 1, while wireless traffic between STA 2 and STA 3, which are associated with different APs, is still allowed. If the “All APs in This Subnet” option is used as shown in Fig. 45, AP 1 and AP 2 communicate with each other via an inter-AP protocol to share their STA association information to block wireless traffic among all the STAs.

There are up to 2 security modes:

- **Open System.** No authentication, no data encryption.
- **Static WEP.** WEP (Wired Equivalent Privacy) keys must be manually configured.

According to the IEEE 802.11 standard, WEP can be used for authentication and data encryption. Normally, **Shared Key** authentication is used if WEP data encryption is enabled. In rare cases, **Open System** authentication may be used when WEP data encryption is enabled. The **Authentication**

algorithm setting is provided for better compatibility with wireless client computers with various WLAN network adapters. There are three options available, including Open System, Shared Key, and Auto.

When WEP is enabled by a security mode, the **Key length** can be specified to be **64 Bits** or **128 Bits**. The **Selected key** setting specifies the key to be used as a send-key for encrypting traffic from the local device side to the remote device side. All 4 WEP keys are used as receive-keys to decrypt traffic from the remote device side to the local device side.

NOTE: Each field of a WEP key setting is a hex-decimal number from 0-9, A-F. For example, when the security mode is **Static WEP** and the key length is **64 Bits**, you could set Key 1 to "00012E3ADF".

3.5.2.2. MAC-Address-Based Access Control

The screenshot shows a configuration window for MAC-Address-Based Access Control. At the top, 'Functionality' is set to 'Enabled' via a dropdown menu. Below it, 'Access control type' has two radio buttons: 'inclusive' (which is selected) and 'exclusive'. There is an empty text input field followed by an 'Add' button. The 'MAC address format' is displayed as '00-02-DD-30-03-1E'. At the bottom, there is a table with two columns: 'MAC Address' and 'Delete'.

MAC Address	Delete
00-50-C2-01-96-4D	Delete
00-09-92-01-02-55	Delete

Fig. 46. MAC-address-based access control settings.

With **MAC-Address-Based Access Control**, you can specify the wireless clients (STAs or Bridge Slaves) that are permitted or not permitted to associate with the SMC2582W-B. When the table type is set to inclusive, entries in the table are permitted to associate with the SMC2582W-B. When the table type is set to exclusive, entries in the table are not permitted to associate with the SMC2582W-B.

NOTE: MAC-address-based access control is only available when the SMC2582W-B is in AP or Bridge Master mode.

To deny wireless clients' access to the wireless network:

1. Select **Enabled** from the **Functionality** drop-down list.
2. Set the **Access control type** to exclusive.
3. Specify the MAC address of a wireless client to be denied access, and then click **Add**.

4. Repeat Step 3 for each other wireless client.

To grant wireless clients’ access to the wireless network:

1. Select **Enabled** from the **Functionality** drop-down list.
2. Set the **Access control type** to inclusive.
3. Specify the MAC address of a wireless client to allow access, and then click **Add**.
4. Repeat Step 3 for each other wireless client.

To delete an entry in the access control table:

- Click **Delete** next to the entry.

NOTE: The size of the access control table is 64.

TFTP server IP address:	<input type="text" value="192.168.0.125"/>
MAC ACL file name:	<input type="text" value="MacAcl.txt"/>
<input type="button" value="Download"/>	

Fig.47. MAC ACL download settings.

Instead of manually entering MAC addresses to the access control table one by one, you can prepare a text file that contains all the MAC addresses and put it on a TFTP server, and then command the SMC2582W-B to download the MAC ACL (Access Control List) file from the TFTP server. Fig. 48 shows the contents of a sample ACL file.

```
00-11-22-33-44-50
00-11-22-33-44-51
00-11-22-33-44-52
00-11-22-33-44-53
00-11-22-33-44-54
00-11-22-33-44-55
00-11-22-33-44-56
00-11-22-33-44-57
00-11-22-33-44-58
00-11-22-33-44-59
00-11-22-33-44-5a
00-11-22-33-44-5b
00-11-22-33-44-5c
00-11-22-33-44-5d
00-11-22-33-44-5e
00-11-22-33-44-5f
00-11-22-33-44-60
```

Fig. 48. Sample MAC ACL file.

To download a MAC ACL file from a TFTP server:

1. Specify the IP address of the TFTP server in the TFTP server IP address text box.
2. Specify the name of the MAC ACL file on the TFTP server in the MAC ACL file name text box.
3. Click **Download**.

3.6. Configuring Advanced Settings

3.6.1. Packet Filters

The SMC2582W-B provides layer 2 (Ethernet Type Filters), layer 3 (IP Protocol Filters), and layer 4 (TCP/UDP Port Filters) filtering capabilities. The configuration processes for the filters are similar.

Functionality: whether this filtering capability is **enabled or disabled**.

Policy for matched packets: how a matched packet is processed—**discard or pass**.

To enable a filtering rule: select the check box to the left of the rule.

3.6.1.1. Ethernet Type Filters

Functionality:	Disabled
Policy for matched packets:	Discard
Name	Number
<input checked="" type="checkbox"/> RARP	0x8035
<input type="checkbox"/> ARP	0x0806
<input type="checkbox"/> NetBUI	0xF0F0
<input type="checkbox"/> Novell IPX	0xB138
<input type="checkbox"/> IPX 802.3	0x00FF

Fig. 49. Ethernet type filters settings.

The **Ethernet type** field of the MAC (Media Access Control) header of a packet incoming from the WLAN or Ethernet interface is inspected for filtering. In a rule, specify the hex-decimal Ethernet type number and give the rule a name.

3.6.1.2. IP Protocol Filters

Functionality:	Disabled				
Policy for matched packets:	Discard				
Protocol Number	Source Address	Subnet Mask	Destination Address	Subnet Mask	
<input checked="" type="checkbox"/> 0x01	192.168.0.3	255.255.255.255	192.168.0.5	255.255.255.255	
<input type="checkbox"/> 0x02	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	
<input type="checkbox"/> 0x06	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	
<input type="checkbox"/> 0x11	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	
<input type="checkbox"/> 0x62	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	

Fig. 50. IP protocol filters settings.

The protocol, source address, and destination address fields of a packet incoming from the WLAN or Ethernet interface is inspected for filtering. In a rule, specify the hex-decimal protocol number,

source IP address range (Source IP Address AND Source Subnet Mask), and destination IP address range (Destination IP Address AND Destination Subnet Mask).

A source (destination) IP address range is determined by performing an AND operation on the source (destination) IP address field and the source (destination) subnet mask field. For example, if the source IP address field is 192.168.0.1 and the source subnet mask field is 255.255.255.0, the resultant source IP address range is 192.168.0.0 to 192.168.0.255.

3.6.1.3. TCP/UDP Port Filters

Functionality: Disabled			
Policy for matched packets: Discard			
<input checked="" type="checkbox"/>	80	TCP	HTTP
<input type="checkbox"/>	80	TCP	
<input type="checkbox"/>	80	TCP	
<input type="checkbox"/>	80	TCP	
<input type="checkbox"/>	80	TCP	

Fig. 51. TCP/UDP port filters settings.

The **destination port** field the TCP or UDP header of a packet incoming from the WLAN or Ethernet interface is inspected for filtering. In a rule, specify the decimal **Destination Port**, **Protocol type** (TCP/UDP), and the name of the higher-level protocol (**Application Name**).

3.6.2. Management

3.6.2.1. Basic

Basic	
<input type="checkbox"/>	Telnet management
UPnP	
Functionality:	Enabled
Device friendly name:	SMC2582W-B

Fig. 52. Basic and UPnP settings.

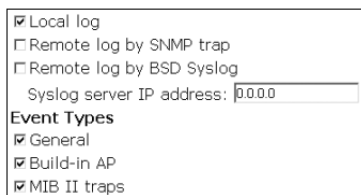
The SMC2582W-B can be managed by Telnet. This functionality can be either enabled or disabled.

3.6.2.2. UPnP

UPnP (Universal Plug and Play) enables a Windows XP user to automatically discover peripheral devices by HTTP. When the UPnP functionality is enabled, you can see the SMC2582W-B in My Network Places of Windows XP. The SMC2582W-B can be given a **user-friendly name** that will be shown in My Network Places. **Double-clicking** the icon in My Network Places that stands for the SMC2582W-B will launch the Web browser for you to configure the SMC2582W-B.

NOTE: Make sure you have installed necessary Windows UPnP components on your Windows XP computer.

3.6.2.3. System Log



System Log settings window. It contains checkboxes for 'Local log' (checked), 'Remote log by SNMP trap', and 'Remote log by BSD Syslog'. Below these is a text box for 'Syslog server IP address' with '0.0.0.0' entered. Under the 'Event Types' section, there are checkboxes for 'General' (checked), 'Built-in AP' (checked), and 'MIB II traps' (checked).

Fig. 53. System log settings.


System events can be logged to the on-board RAM of the SMC2582W-B (Local log) or sent in the form of SNMP trap (**Remote log by SNMP trap**) or **BSD Syslog (Remote log by BSD Syslog)** to a remote SNMP trap monitoring server or remote Syslog server, respectively. See the next subsection for more information about SNMP trap settings. Set the IP address of the Syslog server in the **Syslog server IP address** text box.

The system events are divided into the following categories:

- **General:** system and network connectivity status changes.
- **Built-in AP:** wireless client association and WEP authentication status changes.
- **MIB II traps:** Cold Start, Warm Start, Link Up, Link Down and SNMP Authentication Failure.

NOTE: The SNMP Authentication Failure trap is issued when using an incorrect community string to manage the SMC2582W-B via SNMP and the SNMP MIB II OID, **snmp Enable AuthenTraps**, is enabled (disabled by default).

3.6.2.4. SNMP



SNMP settings window. It includes a 'Functionality' dropdown set to 'Enabled'. Below are text boxes for 'Read-only community' and 'Read-write community', both containing asterisks. The 'SNMP Trap Table' section has a table with two columns: 'IP Address' and 'Community'. The first row is checked and contains '192.168.0.2' and '*****'. There are four empty rows below it, each with a checkbox and the IP address '0.0.0.0'.

	IP Address	Community
<input checked="" type="checkbox"/>	192.168.0.2	*****
<input type="checkbox"/>	0.0.0.0	
<input type="checkbox"/>	0.0.0.0	
<input type="checkbox"/>	0.0.0.0	
<input type="checkbox"/>	0.0.0.0	

Fig. 54. SNMP settings.

The SNMP (Simple Network Management Protocol) functionality can be disabled, and you can specify the name (used as a **password**) of the read-only and read-write community. In addition, up to 5 SNMP trap targets can be set in the **SNMP Trap Table**.

To specify a trap target:

1. Type the IP address of the target host.
2. Type the Community for the host.
3. Select the corresponding check box next to the IP address text box.

Appendix A: Default Settings

TIP: Press the Default switch on the housing of a powered-on SMC2582W-B to reset the configuration settings to factory-default values.

Setting Name	Default Value
Global	
User Name	admin
Password	smcadmin
Host Name	SMC2582W-B
IEEE 802.11b	
Operational Mode	Access Point
Regulatory Domain	FCC (U.S.) or ETSI (Europe)
Channel Number	6
SSID	SMC
SSID Broadcasts	Enabled
Wireless Client Isolation	Disabled
Transmission Rate	Auto
Transmit Power	High
MAC Address	See the label on the housing of the SMC2582W-B.
Security Mode	Open System
WEP Key Length	64 Bits
Selected WEP Key	Key #1
WEP Key #1	00-00-00-00-00
WEP Key #2	00-00-00-00-00
WEP Key #3	00-00-00-00-00
WEP Key #4	00-00-00-00-00
MAC-Address-Based Access Control	Disabled
Access Control Table Type	Inclusive
Link Integrity	Disabled
LAN Interface	
Method of obtaining an IP Address	Set Manually
IP Address	192.168.2.50
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Disabled
Management	
UPnP	Enabled
Device Friendly Name	SMC2582W-B
System Log	Local Log
SNMP	Enabled
SNMP Read Community	public
SNMP Write Community	private
Telnet	Disabled

Appendix B: Troubleshooting

Check the following first:

- Make sure that the power of the SMC2582W-B is on and the Ethernet cables are connected firmly to the RJ-45 jacks of the SMC2582W-B.
- Make sure that the LED ALV of the SMC2582W-B is blinking to indicate the SMC2582W-B is working.
- Make sure the types of the Ethernet cables are correct. Recall that there are two types—normal and **crossover**.

B-1: Wireless Settings Problems

- **The wireless client computer cannot associate with an SMC2582W-B.**
 - Is the wireless client set in **infrastructure** mode?
 - Check the **operating mode** of the WLAN NIC.
 - Is the SSID of the WLAN NIC identical to that of the prospective SMC2582W-B?
 - Check the SSID setting of the WLAN NIC and of the SMC2582W-B.
 - Is the WEP functionality of the prospective SMC2582W-B enabled?
 - Make appropriate WEP settings of the client computer to match those of the SMC2582W-B.
 - Is the prospective SMC2582W-B within range of wireless communication?
 - Check the **signal strength and link quality** sensed by the WLAN NIC.

B-2: TCP/IP Settings Problems

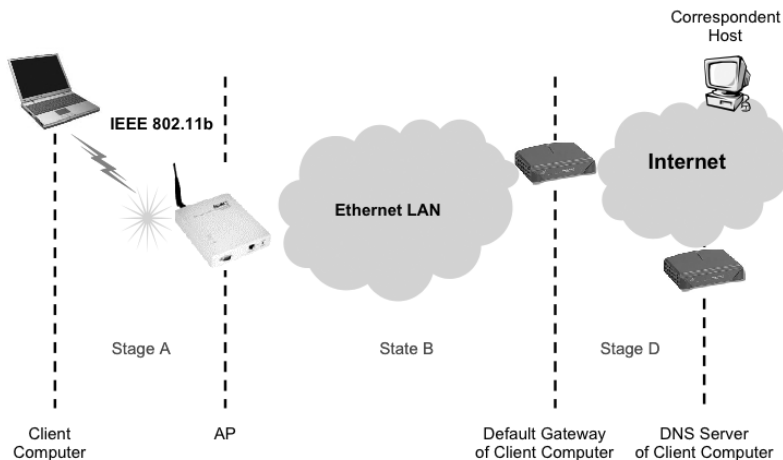


Fig. 55. Communication stages for a client to reach its correspondent host.

For a wireless client computer to communicate with a correspondent host on the Internet by the host's domain name (e.g. <http://www.wi-fi.com>), it first sends a DNS request to a DNS server on the Internet. The DNS request travels first to the AP, then the AP relays this request to the default gateway of the client computer. Finally, this request is forwarded by the gateway to the DNS server on the Internet. The DNS reply issued by the DNS server is transmitted back to the client computer following a reverse path. When the client computer receives the DNS reply, it knows the IP address of the correspondent host and sends further packets to this IP address.

As illustrated in Fig. 55, the communication path could be broken at some of the stages. The OS-provided network diagnostic tool, `ping.exe`, can be employed to find out TCP/IP-related communication problems.

NOTE: If two or more NICs are installed and operating on a client computer, TCP/IP may not work properly due to incorrect entries in the routing table. Use the OS-provided command-line network tool, **`route.exe`**, to add or delete entries from the routing table. Or, use Windows-provided **Device Manager** to disable unnecessary NICs.

Solve the following problems in order:

• **My SMC2582W-B does not respond to ping from the client computer.**

- Are two or more NICs installed on the client computer?
 - Use the OS-provided command-line network tool, **`route.exe`**, to modify the contents of the routing table.
 - Use Windows-provided **Device Manager** to disable unnecessary NICs.
- Is the underlying link (Ethernet or IEEE 802.11b) established?
 - Make sure the Ethernet link is OK.
 - Make sure the wireless settings of the wireless client computer and of the SMC2582W-B match.
- Are the IP address of the client computer and the IP address of the SMC2582W-B in the same IP subnet?
 - Use **`WinIPCfg.exe`** or **`IPConfig.exe`** to see the current IP address of the client computer. Make sure the IP address of the client computer and the IP address of the SMC2582W-B are in the same IP subnet.

• **TIP:** If you forget the current IP address of the SMC2582W-B, use Wireless Router/AP Browser to get the information (see Appendix B-3).

- **The default gateway of the client computer does not respond to ping from the client computer.**

- Solve the preceding problem first.
 - Are the IP address of the SMC2582W-B and the IP address of the client computer in the same IP subnet?
 - If you cannot find any incorrect settings of the SMC2582W-B, the default gateway may be really down or there are other communication problems on the network backbone.
- **The DNS server(s) of the client computer do not respond to ping from the client computer.**
 - Solve the preceding problems first.
 - If you cannot find any incorrect settings of the SMC2582W-B, the default gateway of the SMC2582W-B may be really down or there are other communication problems on the network backbone.

B-3: Other Problems

- **My SMC2582W-B has been set to obtain an IP address automatically by DHCP. How can I know its acquired IP address so that I can manage it using a Web browser?**
 - Use the SMC2582W-B Configuration Utility (WLBrwsr.exe) utility, which is included in the SMC2582W-B Installation CD. This utility can discover nearby SMC2582W-Bs and show their MAC addresses and IP addresses. In addition, it can launch the Web browser on your computer.

NOTE: On Windows 2000/XP, SMC2582W-B Configuration Utility can only be run by a user with administrator privilege.

NOTE: SMC2582W-B Configuration Utility does not scan the SMC2682W.

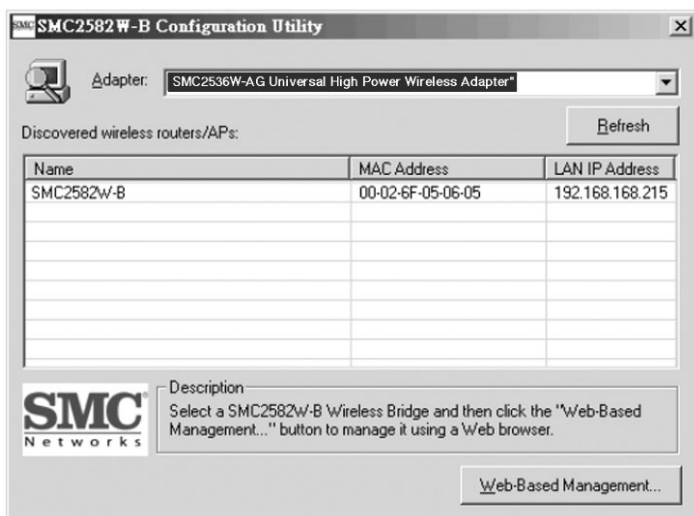


Fig. 56. SMC2582W-B Configuration Utility.

• **My SMC2582W-B stops working and does not respond to Web management requests.**

- The firmware of the SMC2582W-B may be stuck in an incorrect state.
 - Unplug the power connector from the power jack, and then re-plug the connector to restart the SMC2582W-B.
 - Contact our technical support representatives to report this problem.
 - If this happens after a failed firmware upgrade process, the firmware of the SMC2582W-B may have been corrupted.
- If the SMC2582W-B still does not work after restarting, there may be hardware component failures in the SMC2582W-B.
- Contact our technical support representatives for repair.

C-3: Distances and Data Rates

Important Notice: Maximum distances posted below are actual tested distance thresholds. However, there are many variables such as barrier composition and construction and local environmental interference that may impact your actual distances and cause you to experience distance thresholds far lower than those we post below. If you have any questions or comments regarding the features or performance of this product, or if you'd like information regarding our full line of wireless products, you can visit us on the web at www.smc.com or you can call us toll-free at **800.SMC.4YOU**. SMC Networks stands behind this and every product we sell with a 30 day satisfaction guarantee and with a limited-lifetime warranty

IEEE 802.11b Maximum Distance Table				
Environmental Condition	Speed and Distance Ranges			
	11 Mbps	5.5 Mbps	2 Mbps	1 Mbps
Open Environment: A "line-of-sight" environment with no interference or obstructions between Access Point and Users.	160 m (524 ft)	270 m (886 ft)	400 m (1312 ft)	457 m (1500 ft)
Semi-Open Environment: An environment with no major obstructions such as walls or privacy cubicles between Access Point and users.	50 m (164 ft)	70 m (230 ft)	90 m (295 ft)	120 m (394 ft)
Closed Environment: A typical office or home environment with floor to ceiling obstructions between Access Point and users.	25 m (82 ft)	35 m (115 ft)	45 m (148 ft)	55 m (180 ft)

Appendix D: Technical Specifications

D-1: SMC2582W-B Wireless Bridge

Standards:

802.11b
802.3
802.3u
802.3af

Data rate & modulation:

CCK@11/5.5Mbps, DQPSK@2Mbps and DBSK@1Mbps

Radio Technology:

Direct Sequence Spread Spectrum (DSSS)

Operating Range:

Up to 1,500 feet

Frequency range:

2.400 ~ 2.4834 GHz (North America)
2.400 ~ 2.4970 GHz (Japan)
2.412 ~ 2.4720 GHz (Europe ETSI)

Channels:

USA: 1-11 (FCC),
Canada: 1-11 (IC),
Europe: 1-13 (ETSI),
Spain: 10, 11
France: 10-13
Japan: 1-13 (Japan)

Transmission output Power:

18 dBm max

Receiving Sensitivity:

11Mbps 110-5 BER @ -83 dBm, Typical

Antenna:

Removable Antenna with R-SMA connector

Operational Modes:

Access Point/Bridge (used in pure SMC2582W-B bridging environment)
Bridge Master (used when both SMC2582W-B and SMC2682W are in the Bridging environment)
Bridge Slave (used when both SMC2582W-B and SMC2682W are in the Bridging environment)

Interface:

10/100 Mbps RJ-45 Connector
RS-232c Serial Connector
802.11b WLAN

Security:

64/128-bit WEP
MAC address filtering
Disabled SSID broadcast

Configuration and Management

Web-browser
Telnet
TFTP
SNMP
Syslog
Event Logging

LEDs

Power
LAN
WLAN
Alive

Environmental

Temperature: Operating (0~55oC), storage (-20~70oC)
Humidity: 5% to 95% non-condensing in storage

Electromagnetic Compatibility

FCC Class B
Industry Canada
CE
ETS 300.328; ETS 300 826

Dimensions (without antenna):

6.75" x 5.5" x 1.25"

Weight:

0.80 lbs

D-2: SMCPWR-INJ3 Power Injector

Input Power Requirements:

AC Input Voltage	: 90 – 264Vac
AC Frequency	: 47 – 63 Hz
AC Input Current	: 2A at 100Vac, 1A at 240Vac, (-48Vdc)

Power over LAN output Specification:

Pin Assignments and Polarity	: (+) 4/5 (-) 7/8
Output Voltage	: Aggregate Power:50W (48Vdc)

Mechanical Requirement:

Dimensions	: 4" x 5.5" x 1.5"
------------	--------------------

Weight:	: 1.38 Lbs
---------	------------

Indicators:

- System Indicator:
 - AC Power (Green)
 - Power Active (Red) $0.05 A \leq I_o \leq 0.8 A$
 - Over Current Protection (Red, Flash) $I_o \geq 1.0 A$
- Connectors Shielded Rj-45

Environmental Conditions:

Operating Temperature	: 32° to 104° F (0° to 40° C)
Operating Humidity	: Maximum 90% Non-condensing
Storage Temperature	: -13° to 185° F (-25° to 85° C)
Storage Humidity	: Maximum 95%, Non-condensing
Operating Altitude	: -1000 to 10,000 ft. (-304.8 to 3048 m)

Safety Approval:

- UL 1950
- CSA A22.2 No. 950
- EN 60950
- CB

Regulatory Compliance:

- CE Compliance

Electromagnetic Emission and Immunity:

- FCC Part 15 Class B

FOR TECHNICAL SUPPORT, CALL:

From U.S.A. and Canada (24 hours a day, 7 days a week)

(800) SMC-4-YOU; Phn: (949) 679-8000; Fax: (949) 679-1481

From Europe : Contact details can be found on

www.smc-europe.com or www.smc.com

INTERNET

E-mail addresses:

techsupport@smc.com

european.techsupport@smc-europe.com

Driver updates:

http://www.smc.com/index.cfm?action=tech_support_drivers_downloads

World Wide Web:

<http://www.smc.com/>

<http://www.smc-europe.com/>

For Literature or Advertising Response, Call:

U.S.A. and Canada:	(800) SMC-4-YOU	Fax (949) 679-1481
Spain:	34-91-352-00-40	Fax 34-93-477-3774
UK:	44 (0) 1932 866553	Fax 44 (0) 118 974 8701
France:	33 (0) 41 38 32 32	Fax 33 (0) 41 38 01 58
Italy:	39 (0) 3355708602	Fax 39 02 739 14 17
Benelux:	31 33 455 72 88	Fax 31 33 455 73 30
Central Europe:	49 (0) 89 92861-0	Fax 49 (0) 89 92861-230
Nordic:	46 (0) 868 70700	Fax 46 (0) 887 62 62
Eastern Europe:	34 -93-477-4920	Fax 34 93 477 3774
Sub Saharan Africa:	216-712-36616	Fax 216-71751415
North West Africa:	34 93 477 4920	Fax 34 93 477 3774
CIS:	7 (095) 7893573	Fax 7 (095) 789 357
PRC:	86-10-6235-4958	Fax 86-10-6235-4962
Taiwan:	886-2-87978006	Fax 886-2-87976288
Asia Pacific:	(65) 238 6556	Fax (65) 238 6466
Korea:	82-2-553-0860	Fax 82-2-553-7202
Japan:	81-45-224-2332	Fax 81-45-224-2331
Australia:	61-2-8875-7887	Fax 61-2-8875-7777
India:	91-22-8204437	Fax 91-22-8204443

If you are looking for further contact information, please visit www.smc.com or www.smc-europe.com.

SMC[®]
Networks

38 Tesla

Irvine, CA 92618

Phone: (949) 679-8000

Model Number: SMC2582W-B